CLOUDFLARE
AREA 1 SECURITY

# MSSP Onboarding & Deployment Guide

Table of Contents:


**Create Accounts:** **3**
- Create a Parent Account: 3
- Child Account Creation: 5

**Creating users and Assigning permissions:** **7**
- Permissions and Delegated Permissions: 8
- Controlling Parent Access: 9

**Escalation Contacts:** **9**

**Status alerts:** **10**

**Domains Setup (MX/Journaling):** **11**
- Mail flow for MX deployment: 11
- Journaling Setup: 11

**Classification actions:** **12**
- Quarantine: 12
- Message Retraction: 13
- Text Add Ons: 14

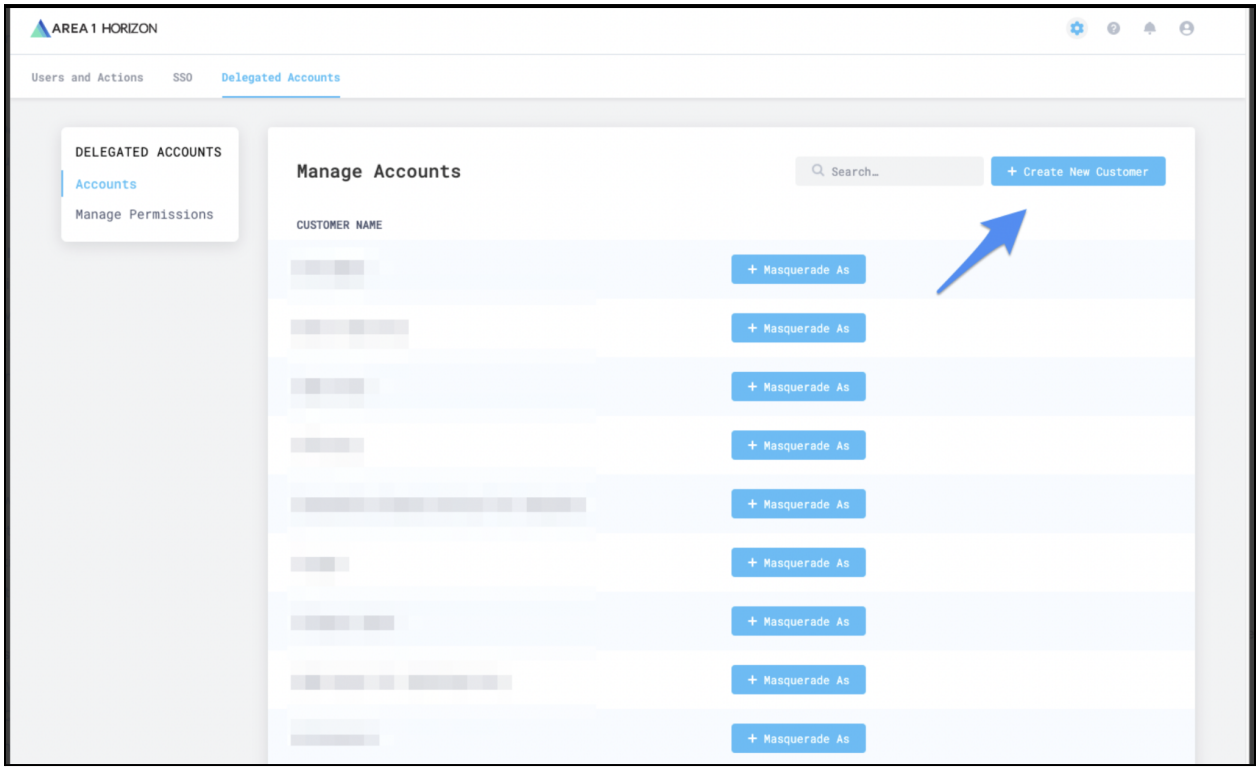
**TLS Enforcement for domains:** **15**
Inbound/Outbound TLS: 15
Partner domain TLS: 16
**Reports:** **17**
Subscribe for weekly and daily reports: 17
SIEM events: 17
**Whitelisting and Blocklisting senders:** **17**
Whitelisting: 17
Blocklisting: 17
**Submitting False Positives and False Negatives:** **18**
False Negatives (missed phish): 18
False Positives: 18
**Area 1 best practices video guides:** **19**

# Create Accounts:

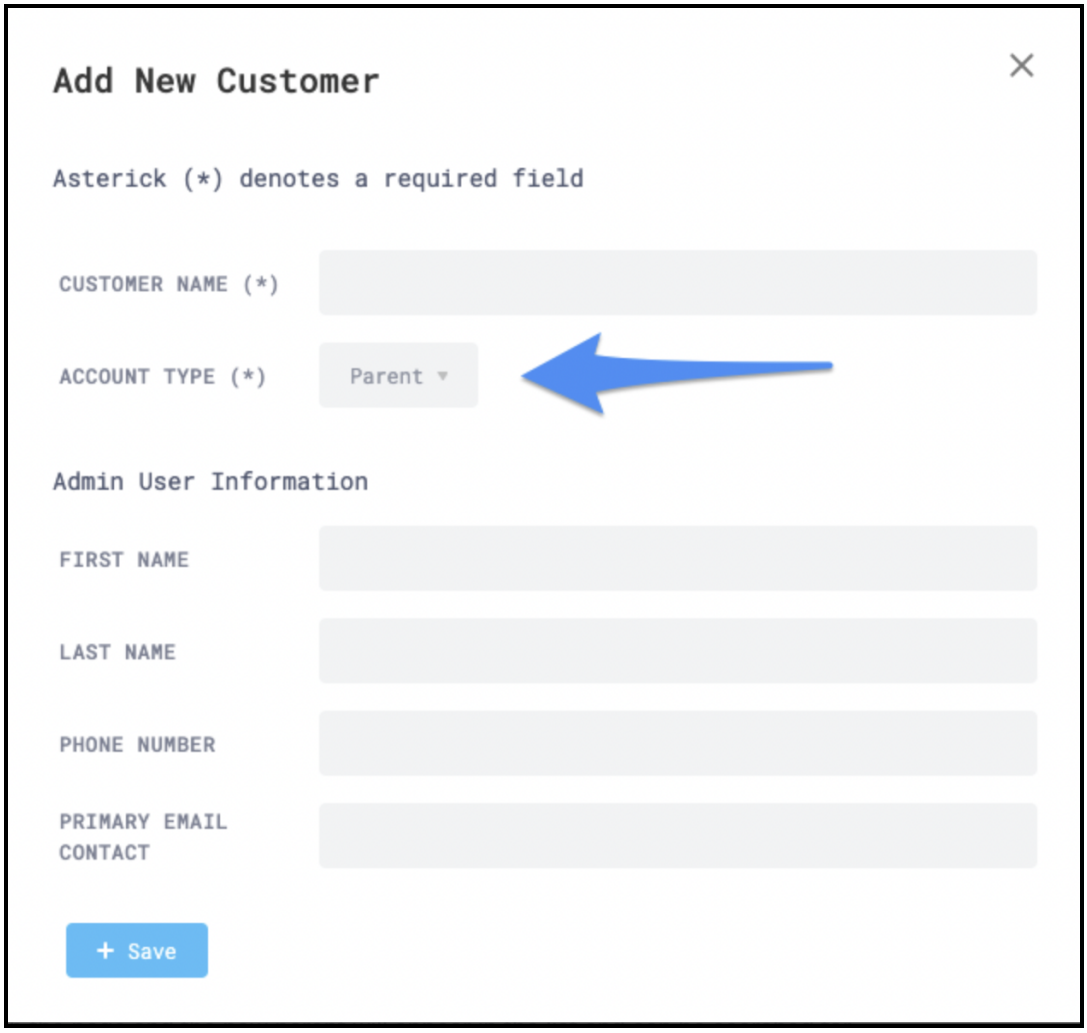
## Create a Parent Account:

Parent accounts are treated as containers with no services provisioned.
User accounts created at the parent level will allow them to access any child account.
**Note:** This is only required for administrators that manage multiple accounts. For ex: MSSP managing multiple customer accounts.

## Parent Creation Process



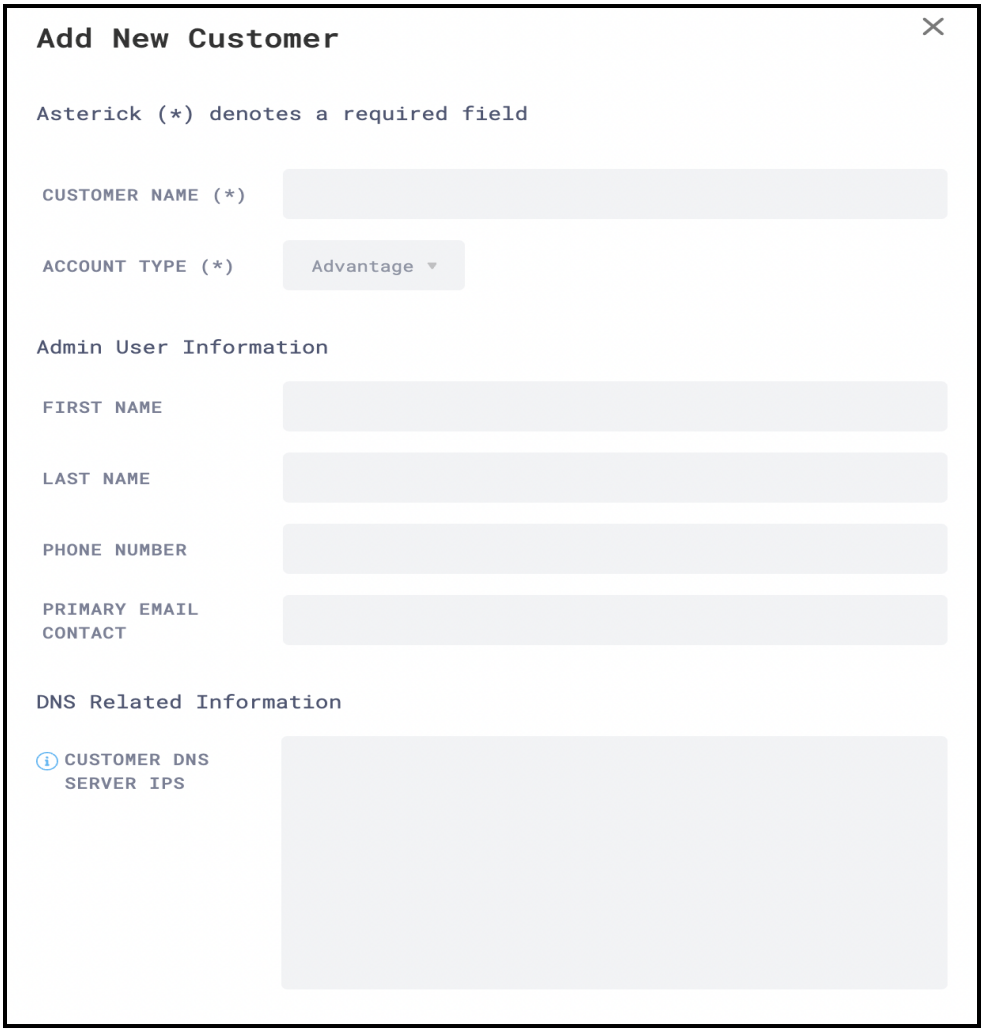

- Login to a Parent Horizon account and visit the **Delegated Accounts** tab.
- Click **Create New Customer** button



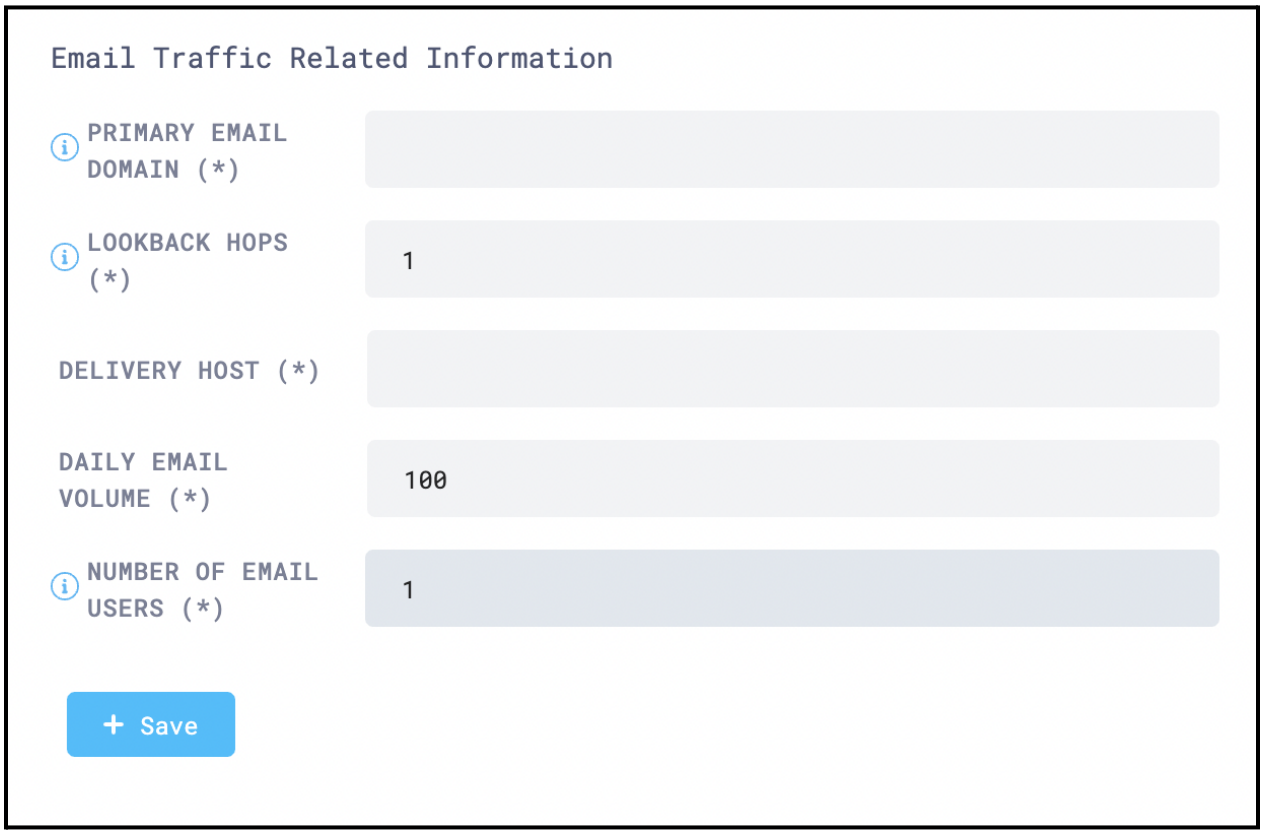

- Select Account Type: **Parent**
- Fill in fields for the **Customer Name**. This will be the name used for the parent and could be a sub-team or other useful name. Names are unique in the system, best practice is to use a descriptive  name that includes your Company and organization purpose. E.g. “Area 1 Security - Parent”, “Area 1 Security - Customers”.
- Click **Save**
- **If the newly created account does not show up in the list of accounts, you can r**efresh the page.

## Child Account Creation:

- Search for a Parent Account from the below link and select the corresponding Parent
  https://horizon.area1security.com/settings/account-delegation/accounts
- Click **Create New Customer** button
- Account Type**: Advantage**
- Fill in the rest of the details for the fields shown in the screenshot below



- At the bottom of the configuration panel enter the email traffic related information.
- Most importantly, please correctly identify and mention the number of email users (users protected by the service).

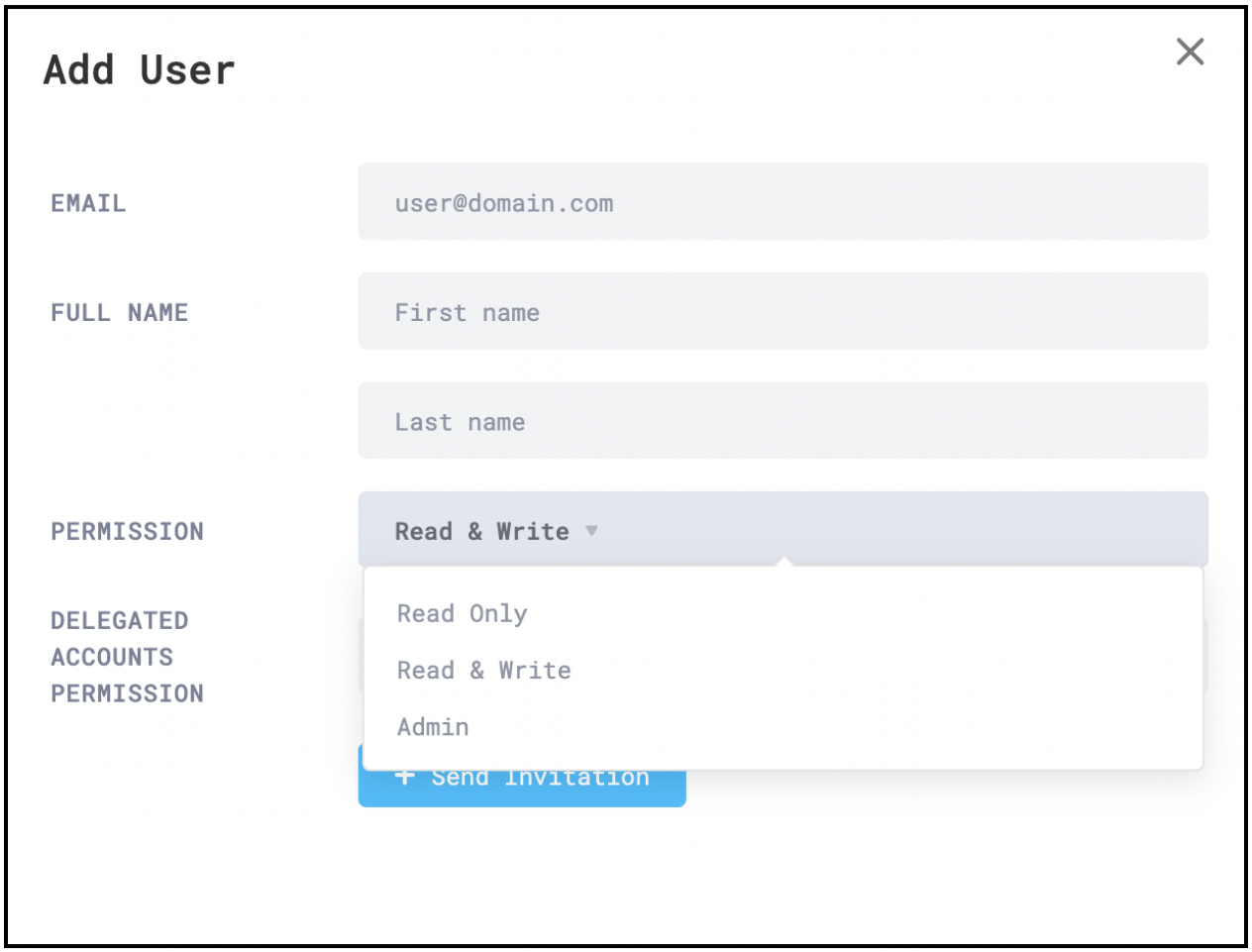


# Creating users and Assigning permissions:

Users can be created at both the Parent and Child account level. Users created at Parent level will have access to all its child accounts. Users created at Child level will only have access to the assigned Child Account. Child Accounts can limit or disable delegated access from the parent. If you modify the Delegated Access controls, ensure you create an Admin account in the Child first.

**Creating User at parent level:**

- Login to a Parent Horizon account and visit the **Users and Actions** tab. https://horizon.area1security.com/settings/users/permissions
- Click on **Add user** button to add a new user and select appropriate permissions
- Click the **+Send Invitation** button. This will generate an email to the user to establish their credential and login to the portal.




**Creating User at Child Level:**

- Log into the corresponding Child Account and follow the same steps as above

## Permissions and Delegated Permissions:

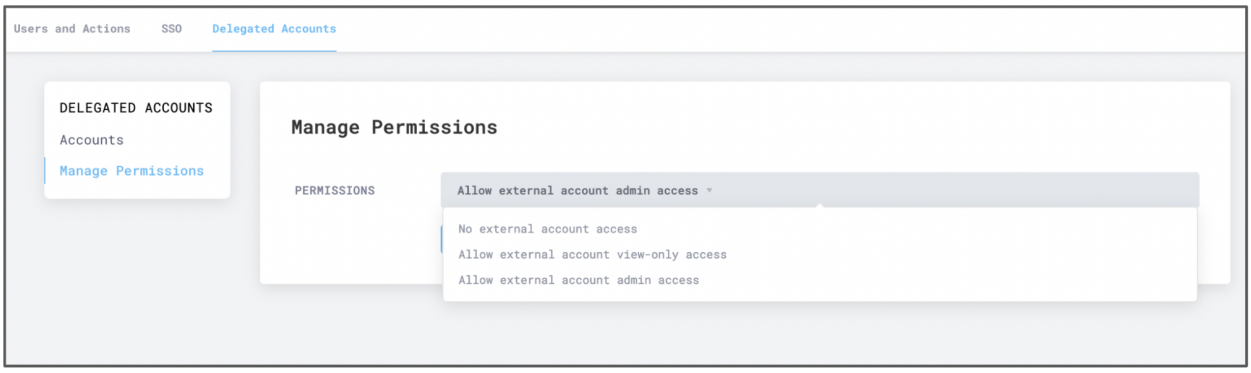
For users of **parent accounts**, they can be designated to have one of following Delegated Account Permission:

- Read-only - > Can enter child accounts but is prevented from making any settings changes, regardless of the customer account settings
- Read-write → Can enter child accounts and make changes on behalf of the customer

For users of **child accounts**, they can be designated to have one of the roles outlined here.

## Controlling Parent Access:

https://horizon.area1security.com/settings/account-delegation/permissions

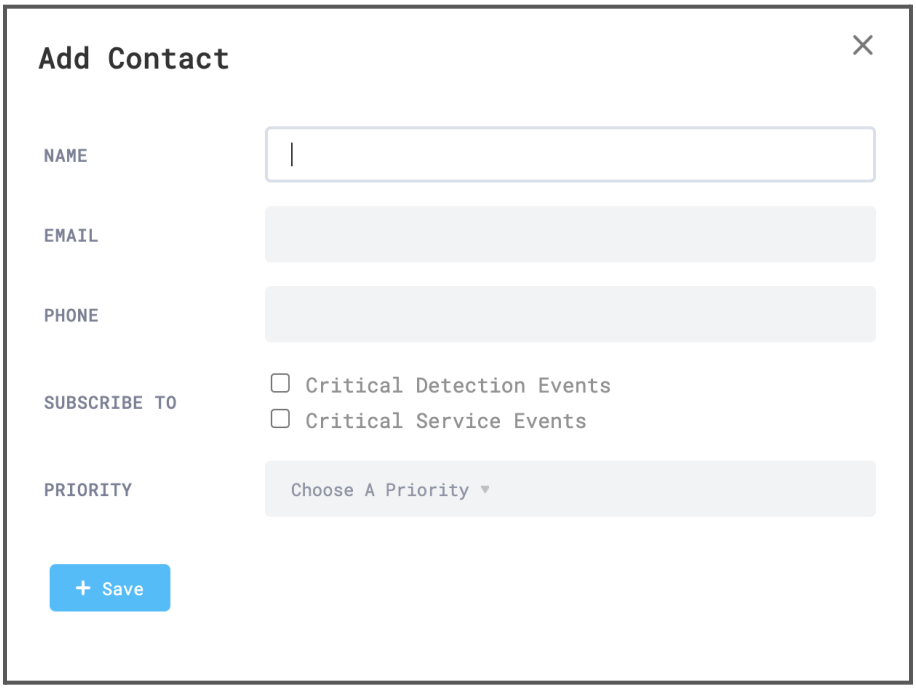



Each child account can set the level of access allowed to their account from the parent.

- No external account access - Shuts off all access from the parent account (including Area 1)
- Allow external account view-only access (Default) - Allows a parent user to view the customer's portal, including settings
- Allow external account admin access - Allows a parent user to administer the customer account on their behalf. By selecting this option the customer is acknowledging consent for outside administration of their account.

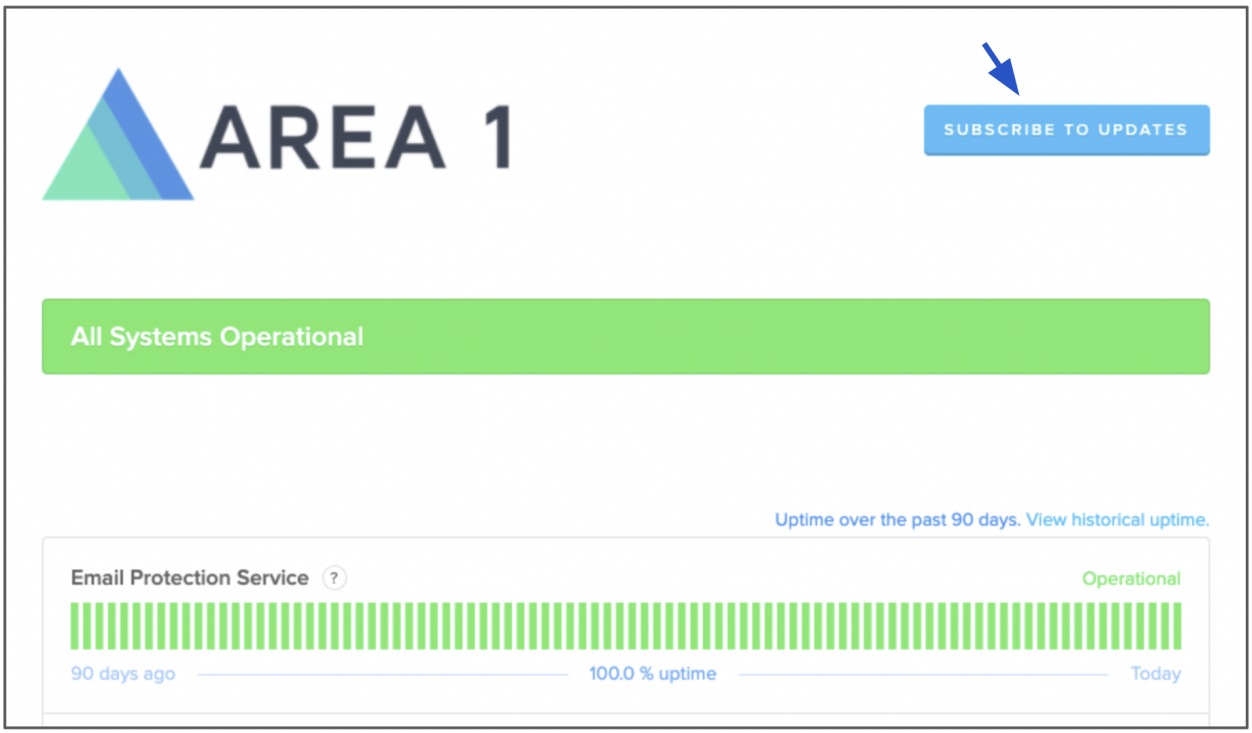
# Escalation Contacts:

- Escalation contacts should be added in order for us to send notifications around Detection events and critical Service related issues. Area1 highly recommends that contacts have both phone and email registered. https://horizon.area1security.com/settings/subscriptions/escalations
- Chose the type of event for which you would like to receive updates and click **+Save**



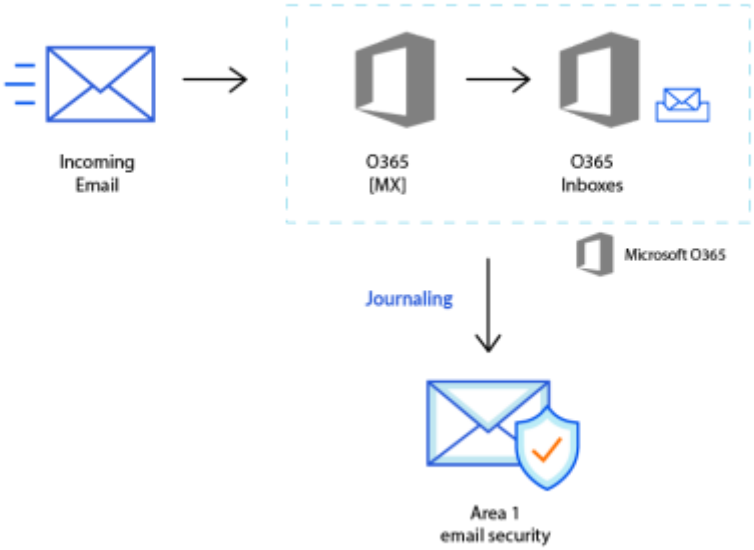
# Status alerts:

Please subscribe to incident status alerts from the following page:
https://status.area1security.com/



# Domains Setup (MX/Journaling):

## Mail flow for MX deployment:




Please reference MX Deployment Setup.

## Journaling Setup:

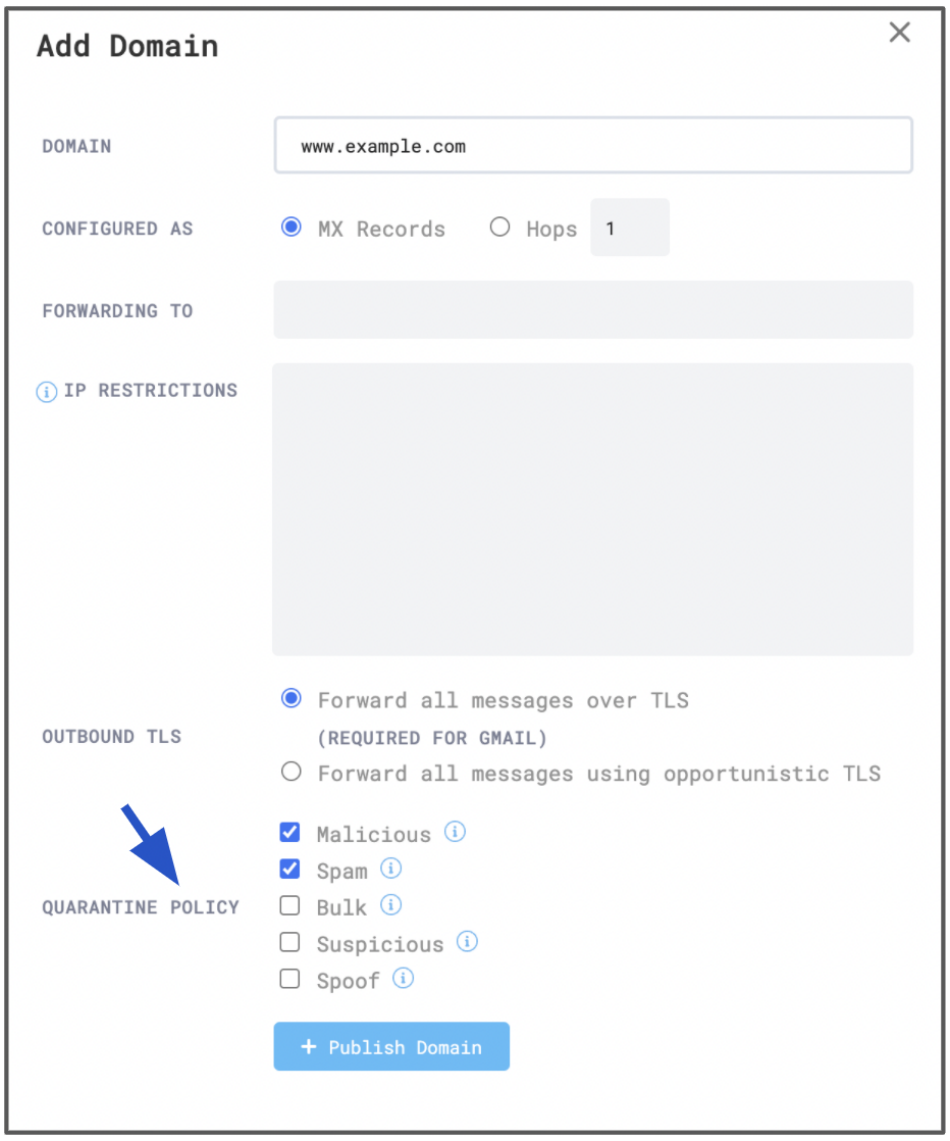
Journaling allows copies of messages to be sent to Area 1 for inspections. This has the benefit to not disrupt your existing email flows. Phishing remediation is accomplished by retracting the offending messages.

Please reference our Journaling Setup docs.

# Classification actions:

## Quarantine:

- We recommend that you quarantine **Malicious and SPAM** dispositions.
- Quarantine can be configured on either O365/GSuite or on Area 1 itself
- Configuring quarantine on Area 1: https://horizon.area1security.com/settings/email/routing/domains



## Message Retraction:

Confidently claw messages out of employee mailboxes, as needed! With Message Retraction, you can take post-hoc action against mail that looks suspect. Please refer to our documentation on **manual retraction**.

**Auto Retraction: (**Auto retraction can be enabled for **Journaling/BCC deployment**.)
**https://horizon.area1security.com/settings/email/retract-settings/automatic-retract**

## Text Add Ons:

- For the dispositions that we do not quarantine (**suspicious, spoof**), we can add text add ons to let the recipients know to work carefully with the emails: https://horizon.area1security.com/settings/email/policies/text-add-ons


We have a different verdict/disposition when we detect a phishing email. Such as Spam, Spoof, Malicious etc. You probably do not want to block all types of detection but want to add some kind of warnings to the email so that end users are aware that the particular email might not be safe.

For such use cases, we have a text add-on feature which will allow you to add warning messages as a prefix to the subject or body of the email.

More details about text add ons.

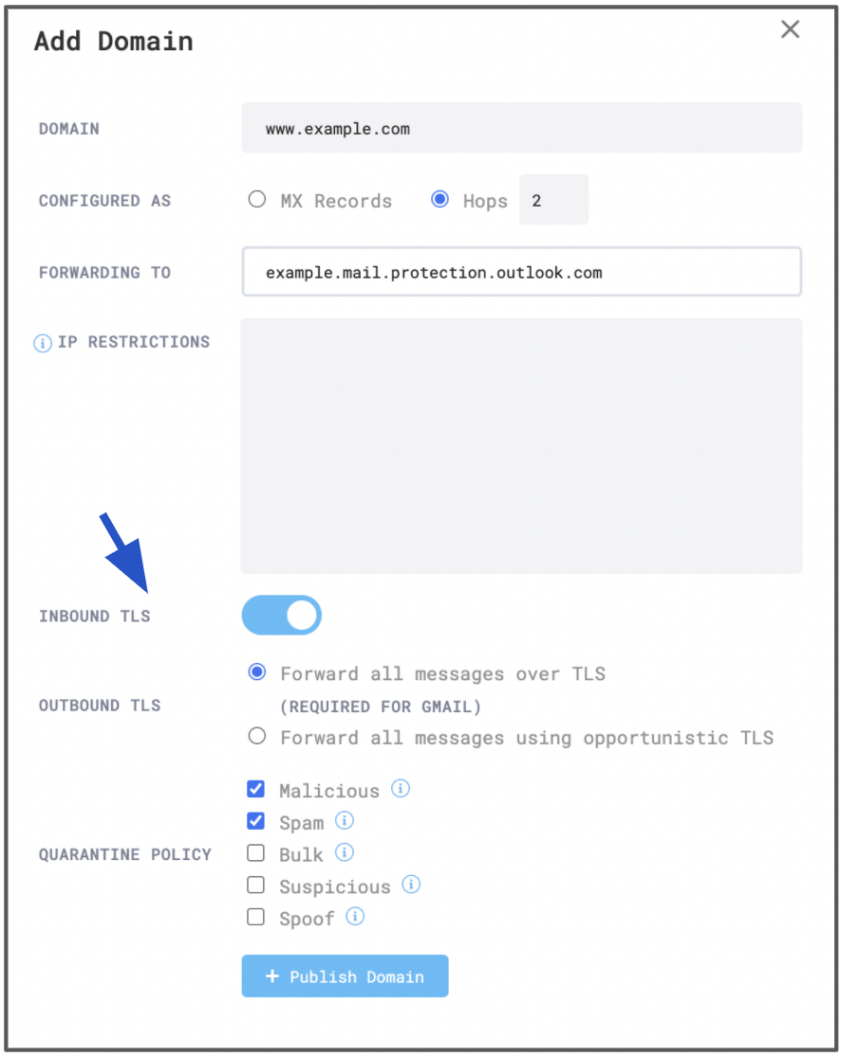
# TLS Enforcement for domains:

## Inbound/Outbound TLS:

https://horizon.area1security.com/settings/email/routing/domains

**Inbound TLS:** Only available for non-MX record domains. This can be either enabled or disabled. If disabled opportunistic TLS is used.

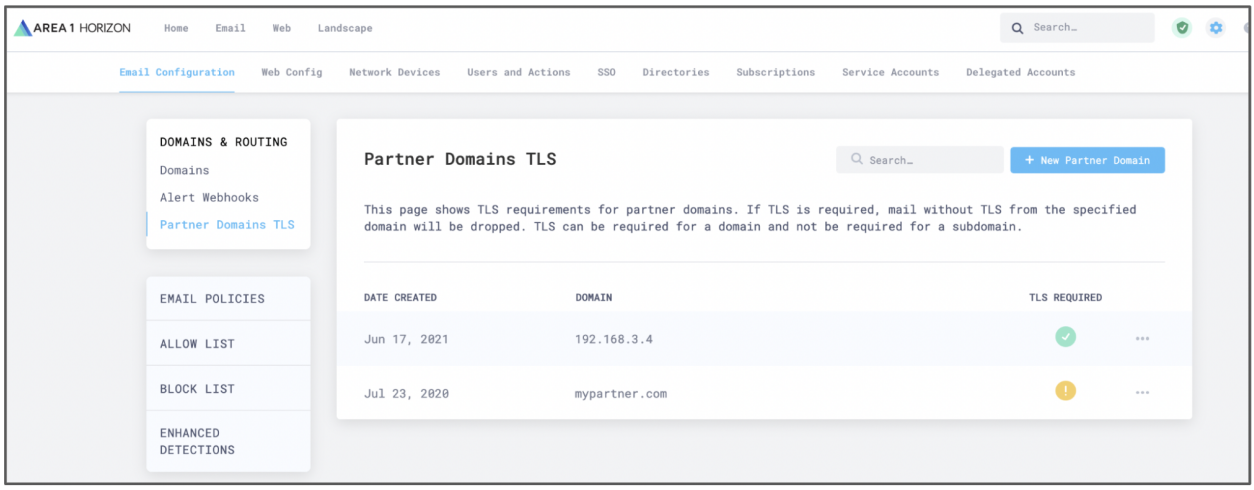
**Outbound TLS:** We recommend that this is enabled to communicate with the next hop (O365/Gmail)



## Partner domain TLS:

As a security control, administrators can enforce TLS for a specific sender domain. When a connection is established, if TLS is required and the sender does not initiate the STARTTLS SMTP verb, the connection will be rejected. This can be defined at the domain and subdomain level.

https://horizon.area1security.com/settings/email/routing/tls-partners



# Reports:

## Subscribe for weekly and daily reports:

https://horizon.area1security.com/settings/subscriptions/email-subscriptions

## SIEM events:

https://horizon.area1security.com/settings/email/routing/webhooks

More details about SIEM integration:
SIEM Integration

# Whitelisting and Blocklisting senders:

## Whitelisting:

https://horizon.area1security.com/settings/email/allow/allow-patterns

## Blocklisting:

https://horizon.area1security.com/settings/email/block/senders

Please refer to the following article for configuration steps:
Allow and block lists

# Submitting False Positives and False Negatives:

## False Negatives (missed phish):

We have allocated a specialized email address for each customer. Please find your addresses here:
https://horizon.area1security.com/support/service-addresses

The above email addresses are provisioned for you to send missed phish directly into our machine learning queue. As soon as you send something it will be automatically processed by our ML module for learning.

Users can also directly report the phish from the O365 client using the 'Report phish' button. Please refer to this article for configuration steps:
Report Phish from Outlook client

## False Positives:

False positives can be reported directly to https://horizon.area1security.com/support/service-addresses.
Please submit either an alert ID or the message ID.

# Area 1 best practices video guides:

1> Allowed Patterns, Trusted domains, Domain age detections

2> Business Email compromise (BEC)

3> Block lists, Text Add Ons

4> Detection search, Mail Trace, SIEM Integration, Email Reports